

【論 説】

相互運用性(interoperability)の 規制法理(序論)

—— 欧州連合のAFSJシステムの
相互運用性立法提案を手掛かりに ——

丸 橋 透

目 次

- 1 はじめに
- 2 欧州の interoperability の用例
 - 2.1 Interconnection/Interlinkage と Direct online (computerized) access
 - 2.2 マーストリヒト条約の inter-operability
 - 2.3 AFSJ データベースの interoperability 提案(2005年)
 - 2.4 小括
- 3 AFSJ システムの Interoperability 提案(2017年)
 - 3.1 提案の経緯
 - 3.2 影響評価書の実装提案の概要
 - 3.2.1 各AFSJシステムの位置づけ
 - 3.2.2 AFSJ各システムへのアクセスの現状
 - 3.2.3 Interoperability 欠如に関する課題と原因
 - 3.2.4 Interoperability 提案の目的
 - 3.3 Interoperability 提案の内容
 - 3.3.1 欧州検索ポータル(ESP)
 - 3.3.2 共用生体情報照合サービス(sBMS)
 - 3.3.3 共通身分情報台帳(CIR)
 - 3.3.4 多重身分検知機能(MID)
 - 3.3.5 法執行目的のヒット-フラグアクセス
 - 3.3.6 Interoperability 実装の全体像
 - 3.4 実装提案から見送られたシステム提案
 - 3.4.1 Prüm システムの改善案
 - 3.4.2 API・PNR システムの中央化案
 - 3.4.3 税関輸入管理システム(CICS)との interoperability 案
 - 3.5 EDPS の意見

- 3.6 提案の現状
- 3.7 小括
- 4 まとめ
- 5 おわりに

1 はじめに

「interoperability」は、多義的あるいは曖昧な概念であり、本稿で主に取り扱う欧州連合の AFSJ (the area of freedom, security and justice) における用例についても magic word⁽¹⁾ あるいは buzz word⁽²⁾ と評されている。それらは、政府が政策推進のために使う際に本来の意図を覆い隠すのに都合が良い言葉である、との否定的なニュアンスを含んでいる。

「interoperability」の定訳は相互運用 (性)⁽³⁾ とされているが、複数のデータベースやシステムを運用する人の側からは、利用時 (つまり人の稼働) の効率性、データベースやシステムの側からも、複数がそもそも稼働している状態であり、その稼働における自動化や効率性の向上を図るという趣旨と捉えれば、相互稼働 (性) との訳も可能ではないかと思われるが、なお検討を要する。

本稿では AFSJ のシステムやデータベースに係る interoperability 又はそれと同一又は関連する概念と思われる用例をまず分析し、2017 年 12 月 13 日に採択された欧州連合の域内治安、国境管理・警備、査証、亡命・庇護、移住の分野における中央情報システムの interoperability の枠組みを定める 2 つの指令案 (以

(1) たとえば Bárd P. '3. Old and new challenges to European criminal justice' (Old & new challenges) In: Carrera, S. and Mitsilegas, V. (Eds.) 'Constitutionalising the Security Union Effectiveness, rule of law and rights in countering terrorism and crime', (Constitutionalising the Security Union) Centre for European Policy Studies (2017) 参照。

(2) たとえば Ballaschk, J. In the unseen realm: transnational intelligence sharing in the European Union-challenges to fundamental rights and democratic legitimacy STAN. J. INT'L L., 2015, 51, 19-51 at 33 参照。

(3) たとえば、鷲江義勝 et al. 欧州同盟条約および欧州共同体設立条約を改定するリスボン条約 (翻訳) (二) 同志社法學, 2008, 60, 1567-1674 においては欧州同盟運営条約 170 条、171 条中の interoperability の訳として「相互運用」を用いている。

下「指令案」)⁽⁴⁾とその共通の影響評価書 (以下「影響評価書」)⁽⁵⁾ (以下あわせて「Interoperability 提案」という) に関する検討を通じて、政策促進概念としての interoperability とそれを規制する法理について考察する。

2 欧州の interoperability の用例

以下、欧州における AFSJ の interoperability 又は類似の概念における規制法理を検討する。

2.1 Interconnection/Interlinkage と Direct online (computerized) access

1987 年 9 月 17 日に欧州評議会の閣僚委員会で採択された警察分野における個

(4) Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on establishing a framework for interoperability between EU information systems (borders and visa) and amending Council Decision 2004/512/EC, Regulation (EC) No 767/2008, Council Decision 2008/633/JHA, Regulation (EU) 2016/399 and Regulation (EU) 2017/2226 COM/2017/0793 final - 2017/0351 (COD) 及び Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on establishing a framework for interoperability between EU information systems (police and judicial cooperation, asylum and migration) COM/2017/0794 final - 2017/0352 (COD)。それぞれ修正提案 (COM/2018/478 final 及び COM/2018/480 final) が提出されている。

(5) COMMISSION STAFF WORKING DOCUMENT EXECUTIVE SUMMARY OF THE IMPACT ASSESSMENT Accompanying the document PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND THE COUNCIL on establishing a framework for interoperability between EU information systems (borders and visa) and amending Council Decision 2004/512/EC, Regulation (EC) No 767/2008, Council Decision 2008/633/JHA, Regulation (EU) 2016/399 and Regulation (EU) 2017/2226 and PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND THE COUNCIL on establishing a framework for interoperability between EU information systems (police and judicial cooperation, asylum and migration) SWD/2017/0474 final - 2017/0351 (COD) 翻訳として丸橋透「域内治安、国境及び移住分野の EU 中央情報システム間の相互運用性の枠組みを定める欧州議会と理事会の 2 つの指令案の影響評価書 (委員会スタッフ作業文書) SWD/2017/0473 final 及びその要旨 SWD/2017/0474 final [参考訳]」法と情報雑誌, 2018 3(3), 201-300 頁。

人データの利用に関する勧告 No. R(87) 15 (以下勧告 (87)15)⁽⁶⁾ の原則 5.6「ファイルの相互接続及びファイルに対するオンラインアクセス」の第 1 副項では、

「異なる目的のために保有されているファイルとファイルの相互接続は、以下のいずれかの条件に従う：

- a. 特定の侵害行為の捜査の目的のための監督官による承認の付与；または、
- b. 明確な法律条項の遵守。」

としている。

ここでは、異なる目的のために保有されているファイルの相互接続(interconnection)の場合には、監督官の統制又は明確な法律条項の遵守が原則とされている。

勧告 (87)15 の説明覚書 (Explanatory Memorandum) 78 項と 79 項によると相互接続は (collect data by) “linking up its files with” (files held for different purposes) と解説され “interlinkage” と言い換えられている。このファイルと他分野のファイル⁽⁷⁾ の interconnection 及び interlinkage が警察分野を含む個人データベース間の interoperability 概念に相当すると思われる。勧告 (87)15 はその統制手段としてデータ保護監督官の事前承認 (a 号)、又は法定 (b 号) を要求する。

一方、第 2 副項では

「ファイルの直接的なオンラインのアクセスは、この勧告の原則 3 ないし原則 6 を考慮に入れた国内立法に従っている場合にのみ、許容されるものとしなければならない。」

とし、他目的のデータベースの直接的オンラインアクセスについては法定による統制を原則として、原則 3 (データの記録保存における一般的な行政文書との分別等)、原則 4 (警察目的に限定したデータ利用) 原則 5.6 以外の原則 5 (他の公的組織、民間、外国の警察組織への送信等) 原則 6 (データ主体のアクセス権、訂正・削除権) 等の統制を要求する。

(6) Recommendation No. R(87) 15 of the committee of ministers to member states regulating the use of personal data in the police sector 翻訳として夏井高人「警察分野における個人データの利用に関する勧告 No. R(87) 15 [参考訳]」法と情報雑誌 1(6) 140-149 頁参照。

(7) 説明覚書には social security bodies, passenger lists kept by airlines, trade union membership file が例示されている。

こちらは、他のデータベースへの直接アクセスを認める場合にその後の利用を統制する考え方であり、個別事案における検索結果を応答する **interlinkage** とは区別していると思われるが、**interoperability** により他のデータベースへのアクセスが認められる場合の事後統制としても当然であろう。ほとんどすべての情報が何らかのデータベースに収納されていることを前提とすると、逆に個別事案におけるファイル間の **interlinkage** が想定しにくい、インターポールの盗難紛失旅客データベース (SLTD) への照会作業のようなものはフルアクセスに至っていないと整理するという考え方もできる。

いずれにせよ、バッチ処理のような個別のデータ抽出要請形態から、他のデータベースのオーナーとしてのフルアクセスまでには至らないデータベース利用形態を可能にする状況を **interoperability** として観念することができそうだ。そして一旦 **interoperable** になってしまった後は、他分野のデータベースから入手した情報の利用については、自己の情報と同等 (以上) の統制が働くことでよいことになる。

他目的 (他分野) のデータベースにフルアクセスできる状態は、データベースあるいはデータベースを収容しているコンピュータシステム同士を結合させることと同等である。なお **interconnection** は、システムが自動的に他のシステムに問合せ、人の手や判断を介さずデータベースを自動更新できる状態の意味で用いられることもある⁽⁸⁾。

2.2 マーストリヒト条約の **inter-operability**

欧州連合の機能に関する条約 (TFEU) 第 170 条第 2 項並びに第 171 条第 1 項及び第 3 項にも **interoperability** 概念が明記されている。これはマーストリヒト条約により追加された条文 (第 129b 条第 2 項並びに第 129c 条第 1 項及び第 3 項)⁽⁹⁾ である。

Trans-European Networks の文脈で構成国の鉄道、道路、通信やエネルギーのネットワークの相互稼働の趣旨であり、「**interconnection**」とは区別した概念として使われている。欧州連合が実装すべき措置として、特に技術標準化を例示して

(8) 上級専門家報告書・後掲注 36 28 頁参照。

(9) 追加時の用語はハイフン付きの「**inter-operability**」であった。

いる⁽¹⁰⁾ので、どちらかというと条約上はネットワーク上の技術的障壁の除去の意味合いが強いと思われる⁽¹¹⁾。

最近の欧州電子通信法 (European Electronic Communications Code) 案⁽¹²⁾においても、**interoperability** は (通信) サービス間で確保すべきもの、との位置付けであり、**end-to-end** の **connectivity** と並んで強化が図られている⁽¹³⁾。

2.3 AFSJ データベースの **interoperability** 提案 (2005 年)

AFSJ データベース間の **interoperability** を確保しようとする欧州連合の試みは 2005 年にもあった⁽¹⁴⁾。

欧州委員会の「司法及び内務分野のデータベース間の向上された効果、強化された **interoperability** 及び相乗効果に関する理事会及び欧州議会への通知⁽¹⁵⁾」において SIS II (以下単に「SIS」という)、VIS 及び EURODAC という 3 種の IT システムに焦点を当て、それらの活用が不十分であること、英数字による検索に限界があること、庇護、移民及び査証のデータを域内の安全目的で利用できないこと、

(10) TFEU 第 171 条第 1 項には “...the Union...shall implement any measures that may prove necessary to ensure the interoperability of the networks, in particular in the field of technical standardization” とある。

(11) 欧州連合の一次法上の **interoperability** の用例としては、他に「欧州連合条約第 42 条により確立される恒常的組織協力に関する第 10 議定書」第 3 条第 c 号に “take concrete measures to enhance the availability, interoperability, flexibility and deployability of their forces, in particular by identifying common objectives regarding the commitment of forces, including possibly reviewing their national decision-making procedures;” (強調筆者付加) とある。共通外交安全保障政策分野の文書であり、共同の戦力の行使にあたってのリソースの効率的利用を意味すると考えられるが、本稿の対象とする AFSJ 分野の **interoperability** との関係性については今後の検討課題である。鷺江義勝 et al. 欧州同盟条約および欧州共同体設立条約を改定するリスボン条約 (翻訳) (三) 同志社法學, 2008, 60, 2275-2344 では、相互運用性の訳語をあてている。

(12) COM/2016/0590 final - 2016/0288(COD)

(13) Id. たとえば、新設の第 3 条第 2 項第 b 号を参照。

(14) Hert, P. D. & Gutwirth, S. Interoperability of police databases within the EU: An accountable political choice? *Int'l Rev. L. Computers & Tech.*, 20, pp21-35 が詳しい。

(15) Communication from the Commission to the Council and the European Parliament on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs COM/2005/0597 final

生体情報の照合ツールが不足していること等から、既存システム利用の改善、既存システムの追加開発及び新システムの開発、庇護・移民当局からの VIS 及び SIS のアクセスの拡大、治安当局からのアクセス権限の拡大等を提案したものである。

提案の内容もさることながら、表題に含まれている **interoperability** については定義を置いているものの、司法及び内務分野のデータベースにおいて具体的にどのような形態が **interoperable** なのかを明記しなかったことから、批判⁽¹⁶⁾を生んだ。

定義によると「**Interoperability**」は、「IT システムとそれがデータの交換及び情報と知識の共有を可能にすることを支援するビジネスプロセスの能力である。」とされ、「データ交換が法的又は政治的に可能又は求められているかどうかの問題とは切断されている」とされた。

前半部分の注として 2004 年 4 月の「汎欧州電子政府サービスの **interoperability** の枠組み第 1 版」(EIF)⁽¹⁷⁾ の定義を引いておりほぼ同じである。

しかし、後半部分の注も EIF を引用しているが、「切断」に相当する文言では無く、以下のとおりである。

「データを交換するときいかに組織がお互いに影響しあうかの詳細は通常 **interoperability** 枠組みに規定されるが、それは標準と指針の組み合わせである。」

しかし、EIF では、**interoperability** 枠組みは組織間で合意することとなっている。組織間で合意するのでは済まない要素、つまり法的、政治的側面については「切断」されているのでは無く、EIF の定義を借りると含みようがないだけである。

欧州データ保護監督官 (EDPS) はこの点、「**interoperability** は単なる技術的概念ではなく、増大する市民のリスクを理由として、法的・政治的なものとしてみるべきである」として厳しく批判した⁽¹⁸⁾。

Interoperability の概念に法的・政治的側面を含めるかどうかについては様々な議論されてきた⁽¹⁹⁾とされるが、少なくとも司法・内務分野のデータベースの

(16) 前掲注 14・Hart 参照 後掲注 18・EDPS 参照。

(17) European Interoperability Framework for Pan-European eGovernment Services Version 1.0 <http://ec.europa.eu/idabc/servlets/Docd552.pdf> (2018 年 9 月 26 日確認)

(18) Comments on the Communication of the Commission on interoperability of European databases https://edps.europa.eu/sites/edp/files/publication/06-03-10_interoperability_en.pdf (2018 年 9 月 26 日確認)

(19) Structured Account of Approaches to Interoperability, ch 4, Report D4. 1. Future of Identity in the Information Society (FIDIS), 6th Framework Programme,

interoperability を論ずるときに技術的概念のみに限定するのは無理があったということだろう。

EDPS は、また、「2つの異なる目的で設計された2つのデータベースの相互接続により、それらが構築されていない第三のデータベースを提供するとき、データベースの集合化は、“function creep” のリスクを増大し、その結果、目的限定原則に明白に矛盾する結果となる。」とした。**Function creep** は、技術やシステムの（機能の）漸進的拡張により、元来企図された目的を超えて利用され（特にプライバシー侵害に至る）ことを指す。

データベース間の **interoperability** がより緊密な形態で実現される場合の個人データの目的外利用リスクを警告したものである。

2.4 小括

以上、現在も勧告として有効な欧州評議会の勧告 R(87)15 をはじめの手がかりとして **interoperability** の概念と規制原理を検討した。**Interoperability** 概念にバッチ処理、又は個別の照合要請を含めるとすると、データ保護監督官のような監督機関による個別承認も選択肢としてあり得るが、オンラインで接続することが前提となる現代の **interoperability** を政策上推進する際の仕組みとしては無理があり、こと AFSJ 分野のデータベースやシステムについては、**interoperable** なシステム上のアクセスや利用の制限に加えて目的外利用の禁止のような要件を法定することが必須であろう。

さしあたり、**interoperability** は、技術的には多数のシステム、データベースやネットワークが相互に稼働し、業務上必要なデータ交換ができ運用されている状態を指す一方、法的、政治的文脈では、可能となった、修正されたか又は新たなデータの利用に伴う機会と（目的外利用をはじめとする）リスクも同時に含む概念であるといえよう。

European Commission, 2005, pp 19-24 参照 http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp4-del4.1.account_interoperability.pdf (2018年9月26日確認) に詳しい。

3 AFSJ システムの Interoperability 提案（2017 年）

3.1 提案の経緯

長文となるが、影響評価書「1. 本提案の政治的及び法的文脈」の筆者による翻訳⁽²⁰⁾を以下抜粋する。

EU は EU 域内への非正規国境通過の増加、及び一連のテロリストの攻撃により示されたとおり、域内治安への進展し継続する脅威を経験してきた。

EU 市民の利益のため、EU 域外国境をより良く保護し、移住管理を向上し、域内治安を強化するために、特に、個人データの保護を受ける権利を含む基本権を完全に尊重しつつ、EU の情報管理は、より効果的かつ効率的にでき、そうしなければならない。EU レベルにおいて国境警備、入国管理、法執行の官吏に対してそれぞれ人に関する情報を提供するために既にいくつかの情報システムがあり、さらにシステムが開発されているが、しかし、EU の情報管理のアーキテクチャは完全ではない。特に、EU レベルの様々な情報システムは、現在相互運用性 — すなわち、主管行政庁や、職務権限を有する官吏が、彼らが必要とする時と場所において必要な情報を持てるよう、データを交換し、情報を共有することができること — が無い。

2016 年 4 月のより強く賢い国境管理及び治安のための情報システム通知⁽²¹⁾において、委員会は情報システムに関連するいくつかの構造的な短所にいかに対処していくかについてその構想を提示した。2016 年 4 月通知の目的は、いかに欧州連合の情報システムが域外国境管理と域内治安をより強化できるかについての議論を開始するためであった。当該通知は、「最近のテロリストの攻撃は、関連する情報共有を強化することの緊急性を、特にセキュリティ

(20) 前掲注 5。抜粋箇所の注記は、本稿の注記としても使用しており、また本稿における追加注記もあるので原文とは異なる。同翻訳中は interoperability の訳語として「相互運用性」を当てている。

(21) COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Stronger and Smarter Information Systems for Borders and Security COM(2016) 0205 final

チェックに関して関連するデータベースの相互運用性を確保することについて「…」特に示した」と述べる欧州理事会の 2015 年 12 月 18 日の結論⁽²²⁾に回答した。ユンカー委員長は、彼の 2016 年 9 月の連合の状況についての一般教書演説⁽²³⁾の中で、この分野についての緊急の進展の重要性を強調した。

理事会は、その分掌として、同様に本分野における行動の緊急の必要性を認識していた。2016 年 6 月、理事会は、司法と内務分野における相互運用性の解決策を含む情報交換及び情報管理を強化する工程表⁽²⁴⁾を承認した。当該工程表の目的は、実務的捜査を支援し、迅速に前線の実務家 — 例えば警察官、国境警備員、検察官、入国管理官及びその他 — に対して、効果的に協力し、行動するための包括的、時宜にかなう、及び高品質の情報を提供することである。これは、更に、2016 年 12 月、情報システムとデータベースの相互運用性についての引き続き成果提供を呼び掛ける更なる欧州理事会結論⁽²⁵⁾に続いた。

欧州議会も本分野での行動を迫った。その 2016 年 7 月の「委員会の 2017 年作業計画に関する決議」⁽²⁶⁾において、議会は、「必要なデータ保護の安全保障を伴う、EU レベルの強制的情報共有の提案と同時に既存システムを向上させ、開発し、情報隙間に対処し、相互運用性に向けて行動する提案」を呼び掛けた。

(22) European Council Conclusions, 17-18 December 2015 〈<http://www.consilium.europa.eu/media/21669/201512-euco-conclusions.pdf>〉

(23) State of the Union 2016 of 14 September 2016 〈https://ec.europa.eu/commission/state-union-2016_en〉

(24) Roadmap of 6 June 2016 to enhance information exchange and information management including interoperability solutions in the Justice and Home Affairs area ? 9368/1/16 REV 1

[訳注] 英文は <http://data.consilium.europa.eu/doc/document/ST-9368-2016-REV-1/en/pdf> にある。

(25) European Council Conclusions, 15 December 2016 <http://www.consilium.europa.eu/media/21929/15-euco-conclusions-final.pdf>

(26) European Parliament resolution of 6 July 2016 on the strategic priorities for the Commission Work Programme 2017 (2016/2773(RSP))

2016年4月通知及び、それが特定した行動の分野に沿い、域外国境及び治安の分野におけるEUの情報インフラの補強に向けて一定の進捗がなされた。

第一に、委員会は、既存の情報システムを強化し、その便益を最大化する行動を実施した。2016年12月、委員会は、既存のシェンゲン情報システム(SIS)の更なる補強のための提案書⁽²⁷⁾を採択した。並行して、2016年5月の委員会の提案書⁽²⁸⁾に従い、修正されたEurodac — EU庇護指紋データベース(EU asylum fingerprint database)の法的根拠に関する交渉が加速された。VISA情報システム(Visa Information System: VIS)の新たな法的根拠のための提案書も準備中⁽²⁹⁾であり、2018年第2四半期に提出される。

第二に、EUのデータ管理アーキテクチャにおける特定された隙間に対処するための追加の情報システムを提案した。委員会の2016年4月の入国/出国システム(Entry/Exit System: EES)を構築する提案書⁽³⁰⁾に基づき、共同立法者は政治的合意に達し、2017年10月に欧州議会により確認され、2017年11月理事会により公式に採択された。2016年11月には、委員会は、非正規移住及び治安の事前審査を可能にすることによる査証免除旅行者のセキュリティチェックを強化するため欧州渡航情報及び承認システム(European

(27) COM(2016) 883 final. [本稿の追加注記] COM(2016) 883 final は SIS の警察及び刑事司法協力事案についての法案。他に COM(2016) 881 final (違法滞在者の送還)、COM(2016) 882 final (国境検問) の 2 法案が同時に出されている。

(28) COM(2016) 272 final

(29) [本稿で追加注] 提案書は COM(2018) 302 final として 2018 年 5 月 17 日に採択済である。新たな法的根拠とは、VIS に長期滞在査証と居住許可証のデータを追加することの法的根拠のことである。

(30) COM(2016) 194 final. [本稿で追加の注] Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011 OJ L 327, 9.12.2017, p. 20-82 として発効している。翻訳として丸橋透「入国／出国システム (EES) 規則 (EU) 2017/2226 [参考訳]」法と情報雑誌, 2018, 3 (2), 199-332

Travel Information and Authorisation System: ETIAS) の構築のための提案書⁽³¹⁾ も提示した。ETIAS 提案書は共同立法者により現在交渉中である。2017 年 6 月、第三国国民の欧州刑事記録システム (European Criminal Record Information System for third-country nationals: ECRIS-TCN system) も構成国の有罪判決を受けた非 EU 国民の情報交換に関して特定された隙間に対処するため提案⁽³²⁾ された。

第三に、委員会は、2016 年 4 月通知中に提示された相互運用性を達成するための 4 つの選択肢に焦点を当て情報システムの相互運用性に向け作業をした：

- 単一の画面で、いくつかの情報システムに同時に問い合わせ、問い合わせられたシステムから混合された結果を生じさせる一元化検索インターフェイス (single-search interface) ；
- 一のシステムに登録されたデータが自動的に他のシステムから参照されるような情報システムの相互接続性 (interconnectivity) ；
- 生体情報データを保有する異なる情報システムをまたいで検索を可能とする共用生体情報照合サービス (shared biometric matching service) の構築；及び
- 就中、一の個人が異なるデータベース中に多重の本人特定情報により登録されているかどうかを検知する異なる情報システムの英数字データ (たとえば名前及び誕生日のような共通の身分属性を含む) の共通身分情報台帳 (common identity repository)。

2016 年 6 月、2016 年 4 月通知のフォローアップとして、国境、移住及び治安のための EU の中央情報システム間の相互運用性を達成するために、上記選択肢の法的、技術的及び運用上の挑戦を検討するため、委員会は情報システム及び相互運用性に関する上級専門家グループを設置した⁽³³⁾。上級専門家グループは、情報システムの複雑性と断片化を原因とする短所と潜在的な情報

(31) COM(2016) 731 final.

(32) COM(2017) 344 final.

(33) Commission Decision of 17 June 2016 setting up the high-level expert group on information systems and interoperability — 2016/C 257/03.

の隙間を特定し、示すこと⁽³⁴⁾も要請された。目的は、広範かつ包括的な情報管理の景観について、税関当局のそれぞれの役目、責任及びシステムも考慮に入れ、見解を得ることである。委員会の2017年作業プログラム⁽³⁵⁾は、国境管理及び法執行のシステムをより相互運用可能とする意図を発信した。

上級専門家グループの最終報告書は、2017年5月に公開⁽³⁶⁾された。それは、EUの情報システムと相互運用性を強化し、開発するための一連の勧告を記した。EU基本権局、欧州データ保護監督官及びEUテロリズム対策調整官の全てが、その専門家グループの作業に積極的に参加した。それぞれ、基本権とデータ保護の広範な問題が、適切に対処されねばならないことを認識しつつも支持する声明を提出した。上級専門家グループは、以下の3つの相互運用性のための解決策に向けて作業することが必要であり、技術的に実現可能であって、それらは、原則として、実務的成果を提供することとデータ保護の要件を遵守して構築することの双方が可能である、と結論づけた：

- 欧州検索ポータル⁽³⁷⁾；
- 共用生体情報照合サービス；及び
- 共通身分情報台帳。

上級専門家グループの最終報告書は、例えば、プリュム（Prüm）枠組⁽³⁸⁾又は搭乗者名記録（Passenger Name Record）指令⁽³⁹⁾を含む既存システムの実装、及び、例えば長期滞在査証の台帳のような潜在的な新しいシステム

(34) Scoping paper of the high-level expert group on information systems and interoperability [訳注] 上級専門家グループ関連の文書は <http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3435> からダウンロードできる。

(35) COM(2016) 710 final.

(36) <http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=32600&no=1>.

(37) 「一元化検索インターフェイス」の用語は、国内情報システムのために構成国に存在する国内の一元化検索インターフェイスと混同することを回避するため、「欧州検索ポータル」に変更された。

(38) Council Decision 2008/615/JHA. 翻訳として夏井高人「特にテロリズム及び国境を越える犯罪との闘いにおける国境を越える協力の拡大に関する理事会決定 2008/615/JHA [参考訳]」法と情報雑誌 2 巻 2 号 155～181 頁参照。

(39) <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016L0681>

の課題についても指摘した。委員会は、これら及び他の勧告で、提案書を通じた直近のフォローアップの対象でないものについて、評価を実施し、いくつかは調査が委託された。

専門家グループの報告書と勧告に応答して、委員会は、効果的かつ真に治安の良い連合に向けての第7次進捗報告書⁽⁴⁰⁾において、すべての、治安、国境及び移住管理のためのEU中央システムが、基本権を完全に尊重しつつ相互運用可能な国境管理及び治安のためのデータの管理への新たな取り組みを規定した。委員会は、法執行機関によるアクセスのためのより効率化された規則を伴う可能性のある、並行して、関連するすべての治安、国境及び移民移住管理に関する欧州システムを検索することが可能な欧州検索ポータル⁽⁴¹⁾の創設に向けて作業を追求し、これらのシステムのために、共有生体情報照合サービス（可能な場合、ヒット-フラグ立て機能⁽⁴²⁾と共に）及び、共通身分情報台帳を開発する意図を公表した。委員会は、相互運用性に関する立法提案書を可及的速やかに上程する意図を公表した。

本施策は、運用の必要性に対するより大きな簡素化、一貫性、効果性、及び注視を伴う法執行目的の司法及び内務の分野における様々なデータベースへのアクセスのための包括的枠組に関する理事会の求め⁽⁴²⁾に応答する。2017年6月の欧州理事会の結論⁽⁴³⁾は、行動する必要性を繰り返した。2017年6月の司法及び内務理事会の結論⁽⁴⁴⁾に基づき、欧州理事会は、委員会に上級

(40) COM(2017) 261 final

(41) 新たなプライバシー・バイ・デザインのコンセプトであって、全てのデータへのアクセスをデータの存在（不存在）を示す単なる「ヒット/ヒット無」通知に限定することにより制限するもの。

(42) 理事会の常設代表委員会（Committee of Permanent Representatives: Coreper）は、2017年3月2日に、EU入国/出国システムの機関間交渉の開始のために理事会議長国に対し権限を与えるに際し、運用の必要性に対するより大きな簡素化、一貫性、効果性、及び注視を伴う法執行目的の司法及び内務の分野における様々なデータベースへのアクセスのための包括的枠組を提案するよう求めた。〔訳注〕Coreper 議事要約 ST 7177 2017 INIT 〈http://www.consilium.europa.eu/register/en/content/out/?&typ=ENTRY&i=ADV&DOC_ID=ST-7177-2017-INIT〉参照。

(43) European Council conclusions, 22-23 June 2017 〈<https://www.consilium.europa.eu/media/23985/22-23-euco-final-conclusions.pdf>〉

(44) Outcomes of the 3546th Council meeting on Justice and Home Affairs on 8 and 9

専門家グループによりなされた勧告を立法する法律案を、可及的速やかに準備するよう求めた。欧州連合をより治安の良い社会にするための努力を補強するため、基本権を完全に遵守しつつ、委員会は、その2018年度作業プログラム⁽⁴⁵⁾において、情報システムの相互運用性に関する提案書を2017年末までに提示することを宣言した。

3.2 影響評価書の実装提案の概要

3.2.1 各 AFSJ システムの位置づけ

Interoperability 提案の対象となる各 AFSJ システム（データベース）の目的と対象データの範囲は図1のとおりである（以下図8までは影響評価書から引用）。

シェンゲン情報システム（SIS）の場合、人（入国や滞在の拒否；EU 逮捕状、行方不明者、司法手続き共助、慎重な審査）及び物（紛失、盗難及び無効の身分証又は渡航書類を含む）に関する広範な範囲の警報機能を備え、第三国国民のデータだけではなく、EU 市民の情報も収容している。

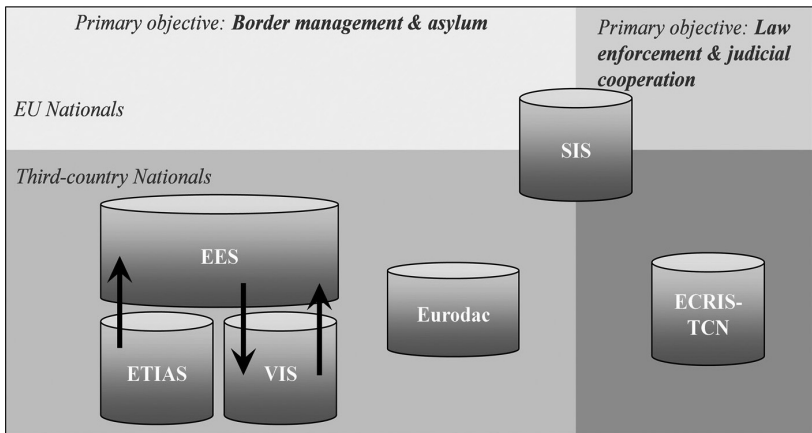


図1：各 AFSJ システムの位置づけ

June 2017, 10136/17 (<http://www.consilium.europa.eu/media/22186/st10136en17-vf.pdf>)

(45) COM(2017) 650 final.

EU 域内の刑事裁判所により第三国国民に対して言い渡された有罪判決についての情報交換をするために新規開発される第三国国民の欧州刑事記録システム (ECRIS-TCN System) は文字通り第三国国民の刑事記録のみを取り扱う。

EU 庇護指紋データベース (Eurodac) は、庇護申請者及び非正規または違法に対外国境を通過し構成国に滞在している第三国国民の指紋データを収容しているが、身分に関する文字情報を追加しようとしている。

新規開発される入国/出国システム (EES) は、現在の旅券の人手によるスタンプ押捺を置き換え、短期滞在のためにシェンゲン圏に来訪する第三国国民の氏名、渡航書類の種類、生体情報及び入国及び出国地点を電子的に登録する。

欧州渡航情報及び承認システム (ETIAS) は、米国の ESTA のように、シェンゲン圏への旅行前に、査証不要第三国国民により提出された情報を集め検証するシステムである。

これまで短期滞在査証のデータを収容してきた VISA 情報システム (VIS) は、長期滞在査証及び滞在許可証のデータも収容することとなる。

3.2.2 AFSJ 各システムへのアクセスの現状

Interoperability 提案の対象である AFSJ システムの他に Interpol のシステムへのアクセスと Europol のデータへのアクセスにおける利用権限者とネットワークの関係の現状を図式化したものが図 2 である。

新設の EES と ETIAS は共通の身分情報台帳を設けることとなっており、入管

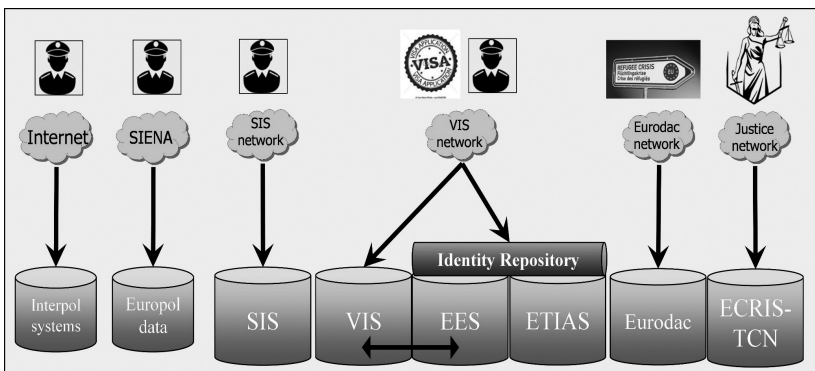


図 2 : AFSJ 各システムへのアクセスの現状

関係者と警察関係者によるアクセスが予定されている。Eurodac と ECRIS にはそれぞれ庇護と検察の当局からの専門のネットワークを通じたアクセスとなる。警察は、SIS と Europol には専門のネットワークを利用し、Interpol のシステムにはインターネット経由でアクセスしている。

3.2.3 Interoperability 欠如に関する課題と原因

委員会の認識した interoperability 欠如の課題は以下⁽⁴⁶⁾のとおりである。

EU 情報システム間の相互運用性の欠如は、利用権限を持つユーザ（国境警備員、法執行官、移民移住管理官、査証担当官又は検察官）の作業を妨げている。

域内治安、国境及び移住の管理のためのデータ管理の（別々のサイロにデータが蓄積されている）断片化されたアーキテクチャは、情報が接続されていないシステムに別々に格納されている場合、EU の域内の治安にとって、盲点に繋がる可能性がある。EU 域外国境の人物に関する管理は、移住の効果的な管理を可能にし、EU 域内の治安に貢献するためにあるべき姿に比して効果的とは言えない。これは、現在進行中の EU への非正規の国境通過及び、一連のテロリストによる攻撃により示されたような域内の治安への脅威の進展により証明されている。

この点に照らし、以下の特定の課題が指摘された：

- 必要な情報への利用権限を持つユーザによる迅速、継ぎ目無く、そして機械的なアクセスの欠如；
- 利用権限を持つユーザが、多重の身分情報及び身分詐称を探知することが不可能なこと；
- 構成国の領域内における身分確認目的での情報システムへの制限されたアクセス；及び
- 国境管理システムに対する様々かつ複雑な法執行機関からのアクセス手段。

これらの課題を引き起こす 4 つの原因が分析されてきた：

(46) 前掲注 5 SWD(2017)474 final の筆者翻訳の A 項の「立法の必要性」から抜粋した。

- 情報システムへのアクセスに関する不適切な構成；
- 法執行機関からのアクセスへの安全保護措置と実務上の必要性の間の不均衡；
- 国境管理システムの目的の制限的解釈
- 個人データの異なるシステム内への、繰り返されかつ別々の保存。

3.2.4 Interoperability 提案の目的

Interoperability 提案により、以下の目的達成を期待した⁽⁴⁷⁾。

2つの一般的な目的：

- 移住に関する欧州議題及びその後のシェンゲンを保全し、強化することに関する委員会通達を含む通達に基づき構築される、シェンゲン域外境界の管理を向上すること。
- 安全保障に関する欧州議題及び、欧州委員会の効果的かつ真の安全保障連合に向けての委員会の作業に基づき構築される欧州連合の域内安全に貢献すること。

4つの特定の目的：

- エンドユーザ、特に国境警備員、法執行官、入国管理官及び検事による、彼らの職務を履行するのに必要な情報に対し迅速、継ぎ目無く、そして統制されたアクセスを、対応する欧州連合の法的文書に規定された既存のアクセス権限を尊重しつつ確保すること。
- 同じ組み合わせの生体情報データにリンクされた多重の身分情報を検知し、善良な（Bona Fide）旅行者の身分確認を促進するとともに身分詐称と闘う二重の目的を有するソリューションを提供すること。
- 構成国の領域における授權された官吏による第三国国民の身分確認を促進すること。
- 重大犯罪及びテロリズムの防止、捜査、検知及び訴追のために必要な場合

(47) 前掲注 5 SWD(2017)474 final の筆者翻訳の A 項の「立法の必要性」から抜粋した。

において法執行官による非法執行情報システムに対するアクセスを促進し、合理化すること。

3.3 Interoperability 提案の内容

以下、Interoperability 提案の具体的な実装内容を概観する。

3.3.1 欧州検索ポータル（ESP）

欧州検索ポータル（European Search Portal: ESP）は個人識別特定データ（身分情報及び生体情報の双方）を利用することによる複数システム（SIS、VIS、Eurodac、ETIAS、ECRIS-TCN システム）の同時検索を可能とする（図3）シングルウィンドウシステムであり、機能的にはデータベースへの問い合わせを媒介するメッセージブローカーである。

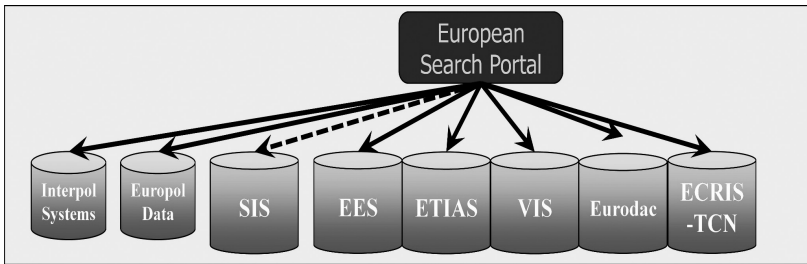


図3：欧州検索ポータル

欧州検索ポータルは新たなデータを取り扱わず、いかなるデータも記録保存せず、かつ、各システムのエンドユーザの既存のアクセス権限を修正しない。SISについては各構成国の国内複製データに対してアクセスされるため中央 SIS に対しては問い合わせがなされない（点線部分）。

3.3.2 共用生体情報照合サービス（sBMS）

共用生体情報照合サービスは生体情報データ（指紋及び顔画像）を SIS、VIS、Eurodac、EES、及び ECRIS-TCN システムから検索することを可能にする（図4）。ETIAS は、生体情報データを含まず、したがって共用生体情報照合サービスにより取り扱われない。SIS、Eurodac、VIS は現在専用の独自の生体情報データ

検索エンジン⁽⁴⁸⁾を有している。共用生体情報照合サービスは生体情報データが同時に検索される共通プラットフォームを提供する。

生体情報（指紋及び顔画像）は、元のシステムに保持されたままである。共用生体情報照合サービスは数値化されたサンプル（検索用特徴点又はテンプレート）を1回のみ生成して保存するが、実データは元のシステムに記録保存したままで、サンプル作成後廃棄される。欧州検索ポータルと同様、共用生体情報照合サービスは、いかなる新しいデータも取り扱わず、エンドユーザのアクセス権限も修正しない。

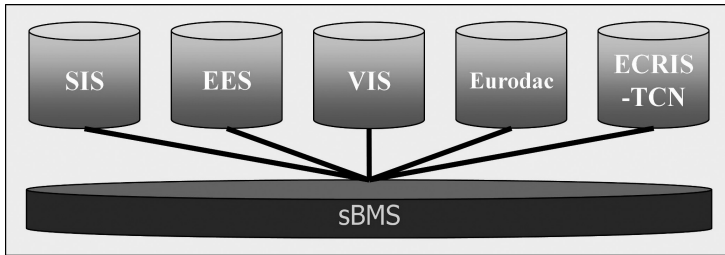


図4：共用生体情報照合機能

3.3.3 共通身分情報台帳（CIR）

共通身分情報台帳（Common Identity Repository: CIR）は、Eurodac、VIS、EES、ETIAS、及び ECRIS-TCN システム中の第三国国民の身分情報データのうち、共通するテキストデータ（姓、名、性別、誕生日、渡航書類番号。住所、以前の氏名、生体情報データ等を含まない。）に関する統一された画面を提供する（図5）。

EESとETIASは共通する身分情報データを共通台帳に記録保存するが、CIRはそれを拡張し、各システムの他の非共通データに紐付ける。

3.3.4 多重身分検知機能（MID）

多重身分検知機能（Multiple Identity Detector: MID）は、ESPを経由した検索に含まれる身分識別特定データが共通身分情報台帳により対象となるシステム（Eurodac、VIS、EES、ETIAS 及び ECRIS-TCN システム）のいずれかあるいは SIS に存在するかどうかをチェックするための機能である。技術的に SIS を共

(48) 技術的には自動化指紋識別システム（automated fingerprint identification system: AFIS）又は自動化生体情報識別システム（automated biometric identification system: ABIS）と呼ばれる。

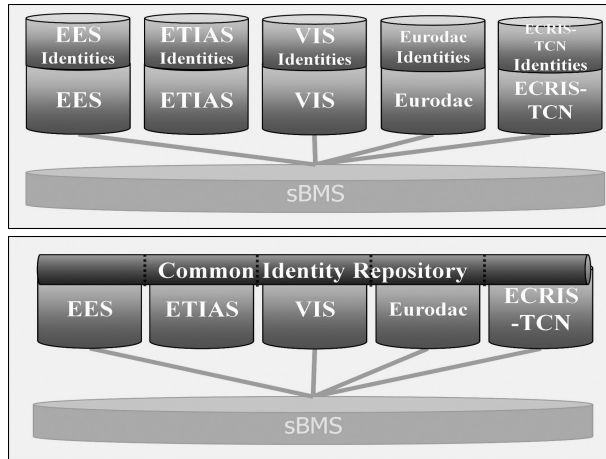


図5：身分情報のサイロから共通身分情報台帳へ

通身分情報台帳に収容することが困難なために設けられる。

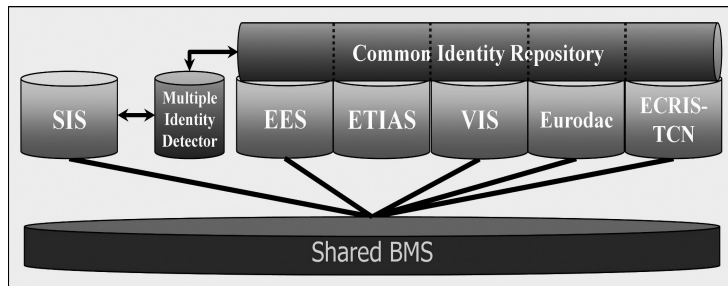


図6：多重身分検知機能

3.3.5 法執行目的のヒット-フラグアクセス

各構成国の警察等の職務権限を有する行政機関が（国境ではなく）領域内で第三国国民の本人確認をする必要がある場合の共通身分情報台帳中のデータへのアクセス権を導入する。

エンドユーザは、身分情報データ（姓、名、誕生日、渡航書類番号）又は生体情報データ（指紋一式及び/又は良い品質の顔画像）の検索を同時並行して CIR（に収容される VIS、EES、Eurodac、ETIAS の身分情報）に対して実行する。する

と、特定のシステムにこのデータが存在するときに「ヒット-フラグ」が返される（図 7-1）。

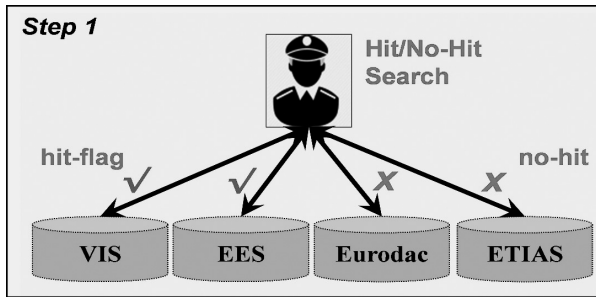


図 7-1：身分確認・法執行目的の HIT-FLAG

第二段階において、かつ必要だと判断されたときにのみ、エンドユーザは「ヒット-フラグ」を提供したシステムへの実際のアクセスを既存のアクセス権及び条件をベースとして要求できる（図 7-2）。システムが「ヒット-フラグ」を返さなかった場合、いかなるアクセスも要求される必要が無い。

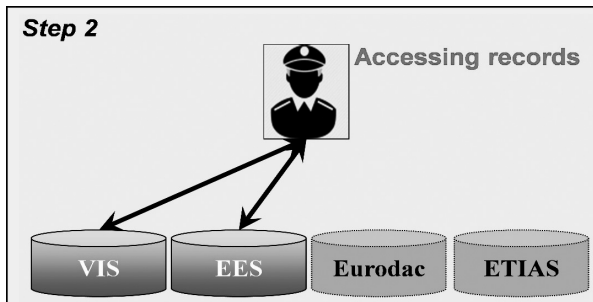


図 7-2 身分確認・法執行目的の HIT した場合のアクセス

「ヒット-フラグ立て」機能は、構成国の職務権限を有する法執行機関が既存の立法の下アクセスすることが許容されないいかなるデータへのアクセスも許容するものではないため、個人データへの新たなアクセスに繋がるものではない。

3.3.6 Interoperability 実装の全体像

Interoperability の各機能の実装提案の全体像は図 8 のとおりである。

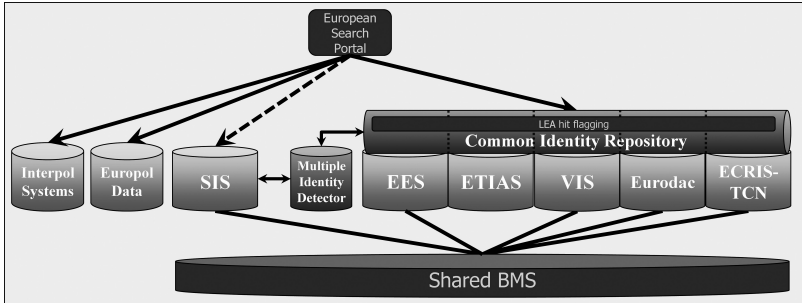


図8：Interoperability 提案の全体像

3.4 実装提案から見送られたシステム提案

2017年5月に公開された上級専門家グループの最終報告書⁽⁴⁹⁾は、Interoperability 提案では見送られたシステムについても提案している。

3.4.1 Prüm システムの改善案

プリュム（Prüm）枠組⁽⁵⁰⁾にもとづく Prüm システムは、各構成国の警察当局が有する DNA、指紋、車両登録情報を相互照会するものである。

上級専門家グループは、現在のメッシュ（Peer to Peer）構成からハブアンドスポーク構成に変更する（図9）ことを提案した（以下図11まで最終報告書より引用）。欧州委員会は eu-LISA と実現可能性の協議を開始している。

3.4.2 API・PNR システムの中央化案

事前搭乗者情報（API）は、現在、各航空会社から各国当局に直接送信されている。今後滞在許可とその期間をチェックするため、EES と ETIAS への自動的なデータ照会が必要になるとき、各国が実装することになる。

上級専門家グループは、API の中央ルーターをたとえば eu-LISA に設置し、航空会社が API データをルーター経由で構成国のシステムに送信するワンストップ ショップ方式（図10）の実現可能性を検討することを推奨した。

上級専門家グループは、各国当局に提出する各航空会社の予約情報の一部である航空搭乗者名記録（PNR）データについても API の中央ルーター経由とすることの実現可能性を検討するよう推奨した。

(49) 前掲注 36 参照。

(50) 前掲注 38 参照。

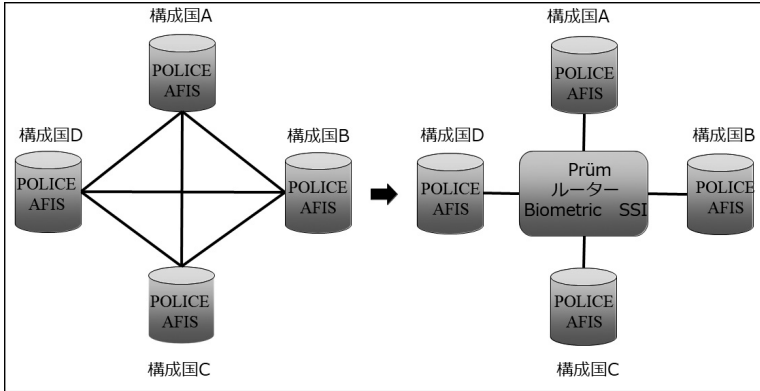


図 9：Prüm システムの改善案

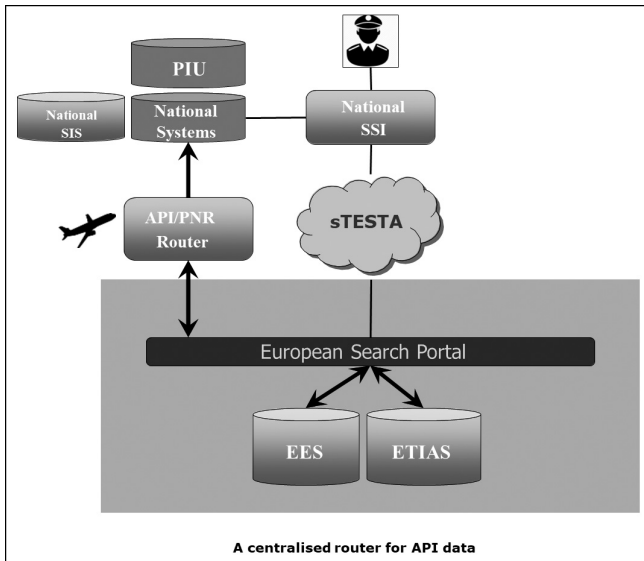


図 10：API・PNR システムの中央化案

この中央ルーター方式は、API・PNR のシングルウィンドウによる航空会社からのデータ受領を日本政府に代わり行っている NACCS⁽⁵¹⁾ と同様のオペレーショ

(51) 輸出入・港湾関連情報処理センター株式会社が提供するシステム。電子情報処理組織に

ンと評価することができ、興味深い。

3.4.3 税関輸入管理システム（CICS）との interoperability 案

上級専門家グループは、税関情報システム（CICS）を治安と国境システムとの間でより相互運用可能となるよう、Europole データを含む関連システムとの連携、さらには欧州検索ポータルを通じたデータ照合（図 11）について別途専門家会合を開催し、実現可能性を検討することを推奨した。

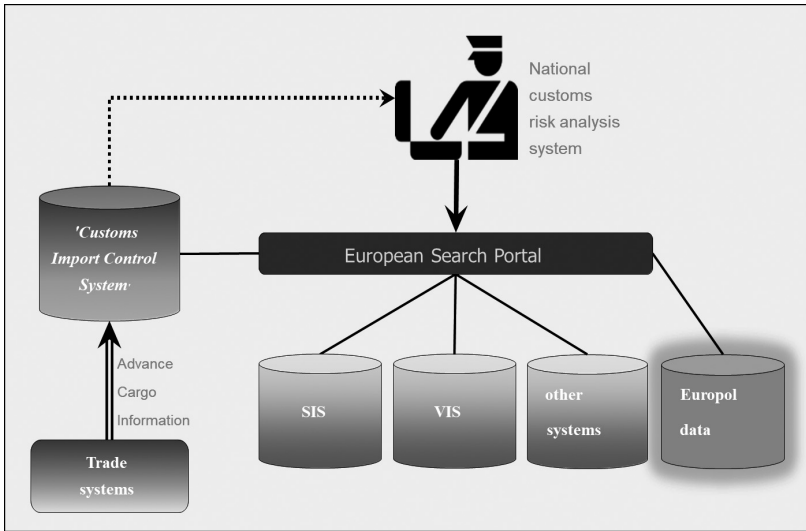


図 11：税関情報システム（CIS）との interoperability 案

我が国の NACCS システムは、通関関連の各種報告・申告サービスを提供しているが、税関への入港前・出港前の報告制度が NACCS システムで運用（又はその予定）がなされており、税関はその情報に基づきテロ物資のリスク分析をしているという。

よる輸出入等関連業務の処理等に関する法律（昭和 52 年法律第 54 号）に根拠を有する政府過半数出資の法人である。

3.5 EDPS の意見

EDPS は、2018 年 4 月 16 日付で提案書への意見⁽⁵²⁾を出した。

EDPS は、上級専門家グループの会合にも参加しており、interoperability 提案の必要性を全否定しているわけではないが、以下を含む意見を述べている。

- interoperability の実現は技術的な選択ではなく、多大な法的・社会的な影響を伴う政治的な選択である。法執行機関に非法執行目的のデータベースに対する定常的なアクセス権を付与することは、大規模 IT システムの構成やその運用に恒久的に影響するだけではなく、この分野の法的原則を変更するおそれがあり、一旦実装されれば引き返せない。したがって、この文脈での将来のデータ交換を統制し、基本権を保護するための幅広い議論が必要である。
- interoperability 提案は、現行（少なくとも立法提案上の差異数段階にあり既に法的に安定している）システムに最後に加える要素という印象を与えるが、実際は、ETIAS, ECRIS-TCN 及び EES）は現在、存在しておらず、SIS と Eurodac は改正議論中であり、VIS は提案されていない。この段階でプライバシーと個人データ保護を精緻に分析するのは不可能である。立法の進捗により、さらなる意見表明をする。
- 提案された手段が適切かつ比例的であることを確保するため、第三国国民による身分詐称（リスク）の程度についてさらに明確化することが重要である。
- 構成国の領域内での身分確認を促進するための各種システムのデータ利用の目的は欧州司法裁判所の判例に従い「厳格に制限され」かつ「精緻に定義」されるべきである。特に CIR へのアクセスは、少なくとも同様の目的で同種の国内のデータベースへのアクセスが認められる場合かつ同じ条件であるべき。
- 提案の実装のあらゆる段階で基本的なデータ保護の原則が考慮されるべきであるので、eu-LISA と構成国はプライバシー・バイ・デザイン及びデフォルトの原則に従うことを明記すべき。

(52) European Data Protection Supervisor Opinion 4/2018 on the Proposals for two Regulations establishing a framework for interoperability between EU large-scale information systems

3.6 提案の現状⁽⁵³⁾

Interoperability 提案については IT システム側の規則提案を反映した修正提案⁽⁵⁴⁾が出されている。

また、Interoperability 提案の対象となる IT システムについての新規・改正立法作業の現在の進捗は、以下のとおりである。

- 入国/出国システム (EES) : 規則発効⁽⁵⁵⁾
- 欧州渡航情報及び承認システム (ETIAS)⁽⁵⁶⁾ : 規則発効
- シェンゲン情報システム (SIS) 強化の提案 : 政治的合意済
- EU 庇護指紋データベース (Eurodac) の法的根拠変更と文字情報の追加 : 難航している模様⁽⁵⁷⁾
- 第三国国民の欧州刑事記録システム (ECRIS-TCN system)⁽⁵⁸⁾ : 政治的合意寸前
- VISA 情報システム (VIS) の強化の法案⁽⁵⁹⁾ : 提出
- AFSJ 分野の大規模 IT システムの運営管理のための欧州連合の部局 (eu-LISA) を設立 (し、AFSJ 分野の大規模 IT システムの運営管理のための欧州の部局 (eu-LISA) と入替え、承継) する規則⁽⁶⁰⁾ : 発効

(53) 2018 年 6 月までの進捗の概況については Communication to the European Parliament, the European Council and the Council: Fifteenth Progress Report towards an effective and genuine Security Union, COM(2018) 470 final にある。翻訳として夏井高人「安全の欧州連合第 15 次進捗状況報告書 COM(2018) 470 final [参考訳]」法と情報雑誌, 2018 3(10) 参照。

(54) 前掲注 4 参照。

(55) 前掲注 30 参照。

(56) Regulation (EU) 2018/1240 of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226 OJ L 236, 19.9.2018, p. 1-71. 規則案は、前掲注 31 参照。

(57) 前掲注 53 参照。

(58) 前掲注 32 参照。

(59) 前掲注 29 参照。

(60) Regulation (EU) 2018/1726 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), and amending Regulation (EC) No 1987/2006 and Council

Eurodac を除き、順調に法案の議論が進んでいると評価できる。

3.7 小括

AFSJ 関連大規模 IT システムの **interoperability** 提案は、専門家会合の運営、EDPS を含む利害関係者の議論への参加等、オープンなプロセスにもとづき、進捗しているといえる。EDPS が指摘する通り、未だ正式に成立していない複数法案、法律として成立していても開発が終了していない複数システムを含む形で提案されている例外的なプロジェクトであり、このプロジェクトや法制度についての最終的に詳細な評価をすることができないが、本稿の目的である **interoperability** の概念と規制法理の観点からは、以下を指摘しておきたい。

まず、テロリズムによる域内治安の強化という課題に対して、情報システムやデータベースの機能及び運用上の短所を明確にすることも当然であるが、課題そのものを明確化することが重要であることである。現行の運用の非効率性、身分詐称や、多重の身分情報の存在がどれほどのリスクを抱えているものなのか等々の諸課題の性質と重みについての精緻な分析があつて初めて、その対策の正当性が評価できる。ICT 投資の費用対効果分析の側面でも必要だろう。

一方、プライバシー、個人データの保護の側面からは、システムやデータベースが **interoperable** で無い状態、つまりサイロ化されている状態は、乱暴な言い方をすれば **interoperable** になるよりはマシ⁽⁶¹⁾、ということになってしまう。しか

Decision 2007/533/JHA and repealing Regulation (EU) No 1077/2011 OJ L 295, 21.11.2018, p. 99-137. 前文 7 に COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS European Interoperability Framework - Implementation Strategy COM/2017/0134 final 及びその ANNEX 2 の指針を適宜参照すること、とある。当該 ANNEX 2 の interoperability の定義(1.1.1)は、‘the ability of organisations to interact towards mutually beneficial goals, involving the sharing of information and knowledge between these organisations, through the business processes they support, by means of the exchange of data between their ICT systems’である。前掲注 17EIF1.0 版と比較すると interoperability を実現するのは ICT システムそのものではなく、それを手段として利用する組織の能力である、とする主役変更がなされている。

(61) Hert・前掲注 14 at pp32 は “The non-interoperability and impermeability of many systems in the past has probably served data protection better than many legal rules with the same goal” と述べる。

し、ICT システムの効率性を向上させてユーザの便益と市民社会の治安リスクを低減することの価値があるのだとすれば、それに伴うリスクをどう低減させるかが知恵の絞りどころである。

Interoperability は目的の異なる大規模システムの統合を回避する手法であるので、EDPS が指摘するような後戻りも場合によって可能ではある。しかし 2005 年通知に対して EDPS が指摘したような **function creep** が行われないう、実装にあたり、元々の利用権限が拡大しないことを確保することが最低限の規律となる。また、ヒット/フラグ立て、のような効率性を確保するための手法は、アクセス権を拡大するものではなくとも、アクセス機会を増大させる。アクセス機会の増大による濫用—**fishing expedition**—のリスクをシステム上及び法制度としてどう抑えるかが問われる。システムへの照合回数の制限や照合ログの事後監査などが、第 1 段階のヒット/フラグ立ての照合作業についても行われる必要がある。

より難易度が高い対策としては、**interoperability** の開発に関するバイ・デザインとバイ・デフォルトの確保であろう。開発の進展につれて各システム自体のリスクが明らかになるときに、たとえばメッセージブローカーに過ぎないシステム側で穴を防ぐのには限界があらう。

4 まとめ

Interoperability は、システムの運用上の効率化とそれによる行政サービス—本稿においては国境審査の効率化とテロリズム対策の強化—の向上という施策を正当化する根拠を表現する方便（**magic word** または **buzz word**）であることは間違いない。したがって、実装する際には、心地よい語感の裏に隠された **function creep** の企図や **fishing expedition** を許容するような設計が無い様、最新の注意を払って専門的な知見を反映した法制度とシステム上の規制をかける必要がある。

さしあたり、規制する法理としては、目的外利用の禁止を維持することが中心となることも間違いない。したがって、利用範囲を元の目的内に抑え込むための、システム上、及び監督、監査上の実装が必要である。

システムを完全統合するのに比べて **interoperability** により生まれるデータの利

用機会の増大の程度は少ないものの、濫用のリスクを抑えるためにはシステム統合の場合に準じた統制手段を検討することが重要な手法になるであろう。

5 おわりに

EU の interoperability 提案を対象として interoperability の規制法理を欧州評議会の勧告 R(87)15 まで遡って検討した。システムの完全統合よりも効率的な政策推進手段としての interoperability は、常に悪であって原則として禁止すべきものである、とまでは言えないものの、予防的な考え方として、interoperability を実装する提案に対しては、その必要性の分析をはじめとして、実装方法とリスク低減のための詳細な検討を要することは明らかである。その観点では、地方自治体の個人情報保護条例に散見される電子計算機のオンライン結合を原則禁止する規定には一定の合理性があると考ええる。つまり専門的知見により外部システムとの interoperability を実装する前のリスク評価ができないのであれば、システムをつながない、という知恵はブリミティブではあるが未だに正しいとも思えるのだ。

今後、さらに歴史をさかのぼり治安分野のシステム、データの結合、オンラインアクセスについての議論を調査すること、他分野における interoperability 事例を比較分析することにより、さらなる知見が得られる可能性がある。大規模 IT システムでの本稿のような分析が、この先の IT システム、究極としては完全な自律性を持った AI 同士の interoperability⁽⁶²⁾ という想像を絶する事態と時代が来るのに備えになるかどうか、システム異常はもちろんのことヒトによる濫用の抑制のためのパイ・デザイン、パイ・デフォルトのシステムと制度の設計思想の在り方（が役に立つかどうかはわからないが、）について研究を進めていきたい。

新美育文先生が座長をされたいくつかの審議会の末席で通信業界側からの勝手な意見を申し上げご面倒をおかけした。丁寧に実務の要請を汲みつつあるべき法

(62) 総務省 AI ネットワーク社会推進会議「報告書 2018—AI の利活用の促進及び AI ネットワーク化の健全な進展に向けて—」（平成 30 年 7 月 17 日）第 3 章 4. AI 利活用原則案の各原則の内容に関する論点の③連携の原則（59 頁以下）及び別紙 3「AI ネットワーク化の進展において想定される課題（ネットワーク化の観点から）」は、自律性を有する AI 間の相互運用性、相互接続性、連携、調整のリスクも検討すべき射程に入っているようではある。

制度をまとめ上げてきた先生のご業績にあらためて敬意を表するとともに、感謝申し上げます。

（2018年9月26日脱稿）

（明治大学法学部教授）